תרגיל בית 1

Wireshark, The Application Layer and Link Delays

שאלה מס׳ 1: Wireshark + HTTP

1. <u>שאלה ממבחן, מועד א׳ סמסטר א׳ 2009:</u>
משתמש הריץ דפדפן (browser) והקיש URL מסוים בשורת הכתובת, בו לא ביקר קודם לכן. בתגובה הוא קיבל דף HTMLהמכיל טקסט ושתי תמונות, שונות זו מזו. כמה קשרי TCP נפתחו בין הדפדפן ושרת ה Web -מרגע הקשת ה URL -ועד להצגת הדף במלואו (כולל התמונות)?
   א. ב-HTTP 1.0?
   משתמשים ב nonpersistent HTTP ולכן כל פעם נשלח אובייקט אחד, סה"כ עבור קובץ ה HTML ועוד 2 תמונות נפתחו בין הדפדפן לשרת **3** קשרי TCP.
   ב. ב-HTTP 1.1?
   משתמשים ב persistent connections כברירת מחדל ולכן נפתח רק **קשר אחד** בין הדפדפן לשרת.

2. מעבדת Wireshark HTTP, חלק 3 (Retrieving Long Documents), סעיפים 12-15.

12. How many HTTP GET request messages were sent by your browser?
הייתה הודעת בקשה HTTP GET **אחת** שנשלחה ע"י הדפדפן
13. How many data-containing TCP segments were needed to carry the single HTTP response?
היו **4** TCP segments שהכילו מידע שנדרש בשביל תגובת HTTP
14. What is the status code and phrase associated with the response to the HTTP GET request?
OK 200
15. Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?
לא

3. מעבדת Wireshark HTTP, חלק 4 (HTML Documents With Embedded Objects), סעיפים 16-17.

16. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
היו 3 הודעות בקשה HTTP GET שנשלחו מהדפדפן לכתובות IP:
128.119.245.12
128.119.240.90
165.193.140.14
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
ע"י בירור מספרי הפורטים בהם היה שימוש בשביל להוריד את התמונות לדפדפן ניתן לזהות אם מדובר בתצורה סריאלית או פרללית , במקרה הנ"ל שתי התמונות עברו בשני חיבורי TCPשונים (בעלי פורטים שונים) ולכן ניתן לקבוע כי התמונות הורדו באופן **סריאלי**.

שאלה מס׳ 2: *Wireshark + DNS*

1. מנו שלוש סיבות עיקריות לכך שאין שרת DNS אחד עולמי. (התייחסו בתשובתכם לגודל, קרבה לאזורים שונים ו-survivability). שימו לב, פירוט כל סיבה מהשלוש לא יעלה על שתי שורות.
   a. לא ניתן לשנות את הגודל של שרת אחד בשביל להתמודד עם **עומס של בקשות** שהולך וגדל עם זמן.
   b. אם יש שרת אחד אז הוא קרוב לאזורים אחדים אך רחוק מאזורים אחרים דבר שיגרור **עומס של תעבורה** אליו.
   c. אם יש רק שרת אחד אז הוא **single point of failure** ולכן כל תקלה או התקפה עליו תשבית את השירות כלומר תפגע ב survivability של השרת

2.
   א. הסבירו בקצרה מה הם:
   - local name server

   שרת DNS מקומי אשר משמש כפרוקסי ומעביר שאילתות מhost כלשהו, לכל ISPיש שרת כזה והוא אינו שייך להיררכיה מסוימת.
   - root name server

   שרת DNSראשי אשר ניגשים אליו שרתי local name server אשר לא מצליחים לתרגם כתובת מסוימת, השרת הראשי מתחבר ל authoritative name server אם המיפוי לא ידוע, משיג את המיפוי ומחזיר אותו ל local name server.
   - authoritative name server

   שרת DNS של הארגון\ISP, מספק מיפוי של hostname ל IP בצורה אמינה לצורכי הארגון כמו שרתי WEBאו דוא״ל

   ב. שאלה ממבחן, מועד ב׳ סמסטר א׳ 2009:

   נתונה היררכיית ה-DNS הבאה:

cis.poly.com מבצע תהליך שאילתת DNS איטרטיבי לגבי gaia.cs.umass.edu.

   א. יש לתאר את תהליך השאילתה האיטרטיבי:
      i. cis.poly.com ינסה לברר בשרת dns.poly.com האם הוא יודע מה כתובת ה IP של gaia.cs.umass.edu במידה וכן הוא יחזיר לו את ה IPהמבוקש ובמידה ולא שרת ה DNS יתחיל בתהליך של בירור הIP עבור ה host
      ii. במידה והכתובת לא ידועה ל dns.poly.com הוא ייגש לשרת ה root וינסה לברר, שרת ה root יגיד לו מי אחראי על הדומין edu כלומר מהו ה IP של dns.edu
      iii. dns.poly.com יפנה לשרת dns.edu בבקשה לברר ויקבל בחזרה את כתובת הIP של dns.umass.edu.
      iv. dns.poly.comיפנה לשרת dns.umass.edu. ויקבל את כתובת הIP של ה host המבוקש
      v. dns.poly.com יחזיר ל cis.poly.com את כתובת ה IP המתאימה של gaia.cs.umass.edu

   ב. נטען כי תהליך שאילתה איטרטיבי עדיף על תהליך רקורסיבי. על איזה גורם מקל התהליך האיטרטיבי (לעומת תהליך רקורסיבי) ולמה?

התהליך האיטרטיבי מקל את העומס מהשרת אליו אנחנו ניגשים בשביל לתרגם את הכתובת, מצב זה מונע מהיווצרות של עומסים על השרתים ברמות העליונות וביניהם ה root name server כלומר מקל עליהם להיות זמינים לשאילתות.

3. בכיתה למדנו על המבנה ההיררכי של DNS, ועל כך שתשובה יכולה לעבור חיפוש רקורסיבי שכולל כמה שרתי DNS בדרך. בסעיף זה נלמד שיטה "לקיצור תהליכים". לצורך כך נשתמש בפקודת nslookup, המאפשרת למשתמש לתשאל שרתי DNS בצורה ישירה, ומציגה את התשובה על המסך.
   א. פתחו חלון פקודות ב-windows (לחצו על Start, בחרו Run, וכתבו cmd בשורת ההפעלה).
   ב. כתבו את הפקודה nslookup www.mit.edu
   מה כתובת ה- IP שקיבלתם בתשובה?
   18.9.22.169
   ג. עתה ננסה לברר מיהו ה- authoritative DNS server כך שנוכל לדבר איתו ישירות. כתבו את הפקודה: nslookup -type=NS mit.edu
   שורה זו אומרת לתוכנית ה-nslookup שאתם מחפשים את כתובת ה-IP של ה authoritative DNS server שאחראי ל-mit.edu domain. **מה קיבלתם?**
   שלושה שרתים:
   bitsy.mit. 18.72.0.3
   strawb.mit.edu 18.71.0.151
   w20ns.mit. 18.70.0.160
   שימו לב, התוכנה מוסרת לכם שקיבלתם את התשובה הזו משרת שהוא non-authoritative. **מה הכוונה בכך?**
   השרת שנתן את המידע אינו אחראי על הדומין הוא רק נותן לנו את האינפורמציה הדרושה בשביל להגיע אליהם, כלומר במקרה הזה הוא רק מראה לנו את השרתים שכן אחראים
   ד. כתבו את הפקודה הבאה:
   nslookup www.mit.edu w20ns.mit.edu
   - מה עושה הפקודה (השוו לפקודה nslookup www.mit.edu)
   הפקודה אומרת לnslookup להשתמש בשרת w20ns.mit.edu בשביל לקבל את המידע על www.mit.edu
   - מה התשובה שקיבלתם?
   Name: www.mit.edu
   Address: 18.9.22.169
   ה. לאור התהליך שעברנו, איך אפשר להשתמש בפקודת ה-nslookup כדי לקצר ואף למנוע חיפוש רקורסיבי בשרתי DNS?
   ניתן לחפש בעזרת הפקודה ע"י שימוש בשרת ספציפי שיבצע את החיפוש וכך להשיג את המידע המבוקש בלי לבצע שאילתות בהרבה שרתים בתהליך וכמובן לתשאל ישירות את השרתים שהם authoritative וכך לקבל תשובה מיידית ללא חיפוש רקורסיבי.

4. בסעיף זה נתייחס להקלטה stanford_web_access.pcap
   ו. בתעבורת ה-DNS הראשונה (בקשה + תשובה), באיזה פרוטוקול השתמשו בשכבת התעבורה? מה הוא ה-port number של אפליקציית ה-DNS בשרת?
   היה שימוש בפרוטוקול UDP בפורט 53
   האם מספר זה הוא Well Known? מה היה ה- type של הבקשה ומה משמעותו?
   כן זהו הפורט המוגדר לDNS ע"פ הפרוטוקול , type A רשומה זו היא כתובת IP (Address)
   ז. בתשובת ה- DNS הראשונה, כמה Resource Records התקבלו? למה?
   התקבלו 3 Resource Records אחד מהם הוא type A והשניים האחרים הם "Canonical name" כלומר שמות נוספים לאותו הדומין.
   ח. הסתכלו על המשך תעבורת ה-HTTP. שימו לב שהדף המבוקש מגיע כאוסף של כמה בקשות HTTP, למשל עבור gifs שונים שמוצגים בו נעשות בקשות HTTP GET חדשות. האם לפני כל בקשה כזו נעשית פנייה חדשה ל-DNS?
   לא.

שאלה מס׳ 3: Link Delays

חבילה עוברת בין שני מחשבים המחוברים ביניהם בלינק ישיר, בנתונים הבאים:

packet length = 3000 Bytes ,Protocol processing time = 80 µsec,
Propagation delay factor = 15 microsec/km ,Channel capacity = 120 Mbpsec
כאשר המחשבים מחוברים בלינק ארוך במיוחד, שאורכו 6000 km (ששת אלפים ק״מ).

(נעזר בשקפים 46-51 מההרצאה הראשונה)
**מזניחים השהיות הנגרמות מעיכוב החבילות בחוצצים (תורים).*

3,000 Bytes = 3,000*8 bits = 24,000 bits

1. How long to format the data?

80 µsec

2. How long does it take a single bit to travel on the link from A to B?

15 / 1000m = t/6000 km
t = 90 µsec

3. How long does it take A to transmit an entire packet onto the link?

120/1 sec = 24,000 bits / t
t = 0.0002 sec (or 200 µsec)

4. What is the <u>total</u> delay?

Total time: 80+200+90+80 = 450 µsec